Section III:	**Application Security**
Title:	**Application Security Controls Standard**
Current Effective Date:	**June 30, 2008**
Revision History:	**June 5, 2008**
Original Effective Date:	**June 30, 2008**

Purpose: To define the elements of security that provides or contributes to system and data availability, integrity, and confidentiality. This standard addresses only the application lifecycle phases of operations and maintenance and disposition.

STANDARD

1.0 Background

Application security encompasses measures taken to ensure the confidentiality, integrity, and availability to the organization's data resources as it pertains to the software used to capture and process that information. Application security attempts to build in controls that protect data resources, detect attempts to breech the security measures, and includes procedures to recover after a threat event has occurred.

2.0 Application Security Assurance

North Carolina (NC) Department of Health and Human Services (DHHS) applications/systems shall implement the appropriate security controls to minimize risk in the production or operating environment based on a risk assessment. The type of controls necessary shall be commensurate with the determination of data confidentiality, integrity, and availability levels. Every application is required to meet ongoing security assurances described in the NC DHHS Security Standards, Administrative Standards - Information Security Certification and Accreditation Standard.

Security testing shall be performed on a periodic basis to ensure that information resources are adequately protected. The Application Security policy applies to all systems/applications. Security testing of all critical information systems shall be performed at least once per year.

Application registration is required for every application where a Division or Office is the business owner. An elaboration of this requirement is discussed in the NC DHHS Security Standards, Physical Standards - Asset Inventory and Control Standard.

Actively maintained application documentation is a critical component to delivering efficient and effective application changes and enhancements. Documentation and user procedures shall be updated to reflect any modification to an application's data structures and/or authorization processes. This documentation shall include, but is not limited to:

- System requirements documents
- System design documents
- Security controls documents
- User manuals
- Operations and maintenance documentation
- Disaster Recovery plans (DR)
- Business Impact Analyses (BIA)
- Business Continuity Planning (BCP)
- System Security plans

2.1 Externally Supported Components

The Division or Office shall properly document provisions that address security concerns as appropriate to the scope and nature of the arrangement to meet legal and business requirements and shall include service level expectations the business owner has of the service provider. An application or components of an application not managed by the application's business owner shall be covered by the same security standards as in-house managed components.

3.0 Change Management Controls

The integrity of the data managed by an application is significantly influenced by the proper operation of that application. To ensure an application is performing correctly, change(s) must be properly managed. More information on managing changes can be found in the NC DHHS Security Standards, Administrative Standards - Information Security Change Management Standard.

3.1 Code Release Management Controls

Code promotion to production must be authorized by management personnel that have determined that predefined standards have been followed. Code review should be done before testing begins. This review shall examine whether the requirements of the change have been fully addressed by the actual code changes.

Program testing must be performed at each stage in the maintenance process. Test cases must include predicted results that will be used and compared to actual results. To ensure availability, both performance and capacity testing must also be performed as required.

Multiple code stage environments must be used during the maintenance process. Those environments are:

- Programmer development
- User acceptance testing
- System testing
- Production environment

4.0 Data Processing Controls

4.1 Controlling On-Line Transactions

When Divisions and Offices accept or initiate on-line transactions, they shall implement controls or verify that controls exist to:

- Validate the identity of the parties involved in the transaction
- Allow proper transaction approval
- Protect confidential data involved in the transaction
- Ensure transaction integrity
- Ensure the transaction completed correctly
- Prevent unauthorized or accidental replay of a transaction.

DHHS Security Standards that provide implementation guidance include: NC DHHS Security Standards, Application Standards - User Authorization and Authentication Standard, NC DHHS Security Standards, Network Standards – Encryption Standard, NC DHHS Security Standards, Network Standards - Telecommunications Security Standard and NC DHHS Security Standards, Network Standards - Digital Signature Standard.

4.2 Routine Application Changes

Routine modifications to an application shall be completed in a way that:

- Minimizes the risk of processing failures that may lead to a loss of integrity
- Can detect any corruption of information through processing errors or deliberate acts

Guidelines:

- Add, modify, and delete functions should be carefully controlled.
- Processes should fail securely such that no further processing will occur. For example, internal controls in processes should be designed to detect if a process is running out of order or without the proper input and fail without further processing.

4.3 Application Operations

To ensure that the results of processing have performed correctly, reports that summarize application activity shall be generated and reviewed by appropriate workforce members. These reports shall be reviewed after every operations cycle.

Guidelines:

- Automatic reconciling of balances from run-to-run or system-to-system can be implemented in systems to compare opening balances against previous closing balances.
- Running hash totals of records or files to be compared run-to-run or system-to-system to ensure that the end of one transaction period is the same as the beginning of the next.

5.0 E-Commerce Controls

5.1 Securing E-Commerce Systems

Divisions and Offices that conduct business via e-commerce shall ensure that information transmitted and/or stored and the supporting information technology are protected by appropriate security measures. In addition, all forms of e-commerce shall comply with any federal, state or Departmental policies, standards, laws or regulations that govern e-commerce.

NC DHHS Security Standards that provide implementation guidance include: NC DHHS Security Standards, Network Standards – Encryption Standard, NC DHHS Security Standards, Network Standards - Telecommunications Security Standard and NC DHHS Security Standards, Network Standards - Digital Signature Standard.

5.2 Using External Service Providers for E-Commerce

When Divisions and Offices contract with external service providers for e-commerce services, the services shall be governed by a formal agreement. All external service providers for e-commerce shall have provisions in their agreements with Divisions and Offices that set forth the requirement that they shall comply with any federal, state, or Departmental policies, standards, laws, or regulations that govern e-commerce or data involved within the e-commerce action.

6.0 Application Availability

The application support team is responsible for ensuring the application continues to meet availability objectives established by business needs. When components of an application are managed by someone other than the Division or Office, the application support team shall review actual performance statistics and the service level agreement (SLA) to ensure the availability needs established by the business owner are being met.

The application support team will maintain and ensure the execution of data backup plans that provide for the recovery of application data due to unforeseen circumstances.

7.0 Data Transmission Controls

Data that enters or leaves the state's network is vulnerable. When those transmissions involve confidential or sensitive data, special precautions are required.

Guidelines:

A communications protocol and/or data software that ensures encrypted secure communications shall be used under the following conditions:

- Client application access originating outside the state network to an application on the state network
- Transfer of information originated by a source outside the state network and a computer on the state network
- Transfer of information from within the State network to a computer not on the state network

Encryption must be used where the transmission of confidential data occurs. Encryption algorithms for the transmission of confidential data include, at a minimum, Secure Socket Layer (SSL) RC4 128 bit algorithms, SSL Server-Gated Cryptography (SGC) 128 bit algorithms, TLS 1.11 128 bit algorithms, or those algorithms that are accepted and certified by the National Institute of Standards and Technology (NIST).

Application owners shall instruct their users about these requirements and publish them in the application's User Manual.

8.0 Access Controls

Divisions and Offices shall restrict access to operating systems and operational or production application software/program libraries to designated staff only. As an application is maintained, care must be taken to ensure the application data access controls are not bypassed and that the principles of least privilege and segregation of duties are preserved.

Access and authorization standards are described in the NC DHHS Security Standards, Application Standards - User Authorization and Authentication Standard.

9.0 Host and Database Software Controls

End user applications can run under the control of one or more operating systems and often interface or use other software products such as a database, web server, reporting tool, etc. The following considerations that shall be addressed to ensure that those supporting elements used by an application are also kept secure.

9.1 Operations Administration

Divisions and Offices shall address and implement the following controls:

- Employ and document controls to provide for the management of system operations and system administration
- Ensure that there is proper segregation of duties to reduce the risk of Division and Office system misuse and fraud
- Develop change control procedures to accommodate resources or events that require changes to system operations as described in the NC DHHS Security Standards, Administrative Standards - Information Security Change Management Standard
- Control access to information resources as described in the NC DHHS Security Standards, Application Standards - User Authorization and Authentication Standard
- Implement a program for continuous monitoring and auditing of systems use to detect unauthorized activity

9.2 Operations Controls

Only diagnostic, configuration, and those ports necessary for the operation of the application shall be active and available. The ports should be controlled and limited to only those with a business need to access the application. All default guest accounts shall be renamed and disabled.

Each Division and Office shall ensure that the operating systems used to run the production environment are regularly monitored for security risks and maintained in approved secure configurations to support business operations.

Additional controls described in the NC DHHS Security Standards, Application Standards - User Authorization and Authentication Standard shall be implemented.

9.3 Software Changes

To maintain the highest level of system availability and protect the Division and Office infrastructure, maintenance operations shall be performed at predetermined, authorized times or on an approved, as-needed basis. Documented operational procedures shall be created, implemented, and maintained during system operations. All changes shall be first applied in a non-production environment similar to the production environment. Testing shall be performed to ensure that the end-user application(s) has not been adversely impacted. Each Division and Office shall manage changes to its systems and application programs to protect the systems and programs from failure as well as security breaches.

Additional change management/change control requirements are outlined earlier in this document in Section 2.0.

9.4 Operating System Upgrades

Operating system upgrades shall be carefully planned, executed, and documented.

9.5 Software Patches

System administrators shall ensure that all current maintenance and security vulnerability patches are applied with reasonable priority and testing is performed prior to release on production servers.

10.0 Audit Controls

As applications are maintained in the operations environment, audit controls shall be implemented and ensured. Audit trail documentation shall include sufficient information to establish what events occurred, when, and who (or what) caused them. Logging shall occur at the network, operating system, and application level. The level of monitoring and logging required for systems and networks shall be determined by a risk assessment. Minimum monitoring and logging standards specified within the Division or Offices policies or standards shall be performed in all cases.

The NC DHHS Privacy and Security Office (PSO) shall assess all production Departmental applications and systems on a regular basis. In addition to application or system-level audits, information system activity reviews shall be conducted or facilitated by the DHHS PSO on a periodic basis. All systems that process sensitive information, or are considered critical to the Department, shall have automated audit control functionality implement.

Divisions and Offices shall designate trained staff to regularly review operational audit logs including system, application, and user event logs for abnormalities. Any abnormalities and/or discrepancies between the logs and the baseline that are discovered shall be reported to management. Management should report recurring abnormalities as a security incident.

System usage shall be monitored and reviewed for activities that may lead to business risks. System and database administrators shall review audit logs to the extent necessary to detect potential security incidents and security breaches.

Access to audit logs shall be protected from unauthorized access, modification, or destruction and shall be reviewed periodically for action. These logs shall be retrievable through clearly defined procedures and shall be maintained for time periods prescribed for audit, legal, and recovery purposes.

11.0 Data Classification

Data shall be appropriately classified as required by the NC DHHS Security Standards, Administrative Standards, Information Classification Standard. When new data elements are introduced to an application, all of the data elements within the application will be re-evaluated and re-classified as necessary.

12.0 System Recovery and Testing

The application support team shall maintain a Disaster Recovery Plan for each application and perform periodic testing according to the schedule published by the DHHS PSO based on the application criticality. Please see the NC DHHS Policy and Procedure Manual, Section VIII - Security Manual - Business Continuity and Disaster Recovery Plan Policy for more information.

13.0 Incident Reporting

The application support team shall report all security incidents as required by the NC DHHS Policy and Procedure Manual, Section VIII – Security Manual - Information Incident Management Policy.

14.0 Application Disposition

The following actions shall be considered when an application has been selected for replacement or decommission:

- Production data shall be archived to meet data retention requirements
- A method is devised that provides for the structural understanding and retrieval of the archived data
- The application registry is updated to remove or note the change in status of the application

Disposal or reuse of data storage media must conform to the NC DHHS Security Standards, Physical Standards - Asset Inventory and Control.

References:

- HIPAA Administration Simplification - Act 45 C.F.R. Part 160 and 164
  - HIPAA Administrative Simplification Act, 45 CFR: § 164.308 Administrative safeguards, (a) (7) (ii) Implementation specifications, (A) Data backup plan.
  - HIPAA Administrative Simplification Act, 45 CFR: § 164.312 Technical safeguards, (a) (1) standard: Access control.
  - HIPAA Administrative Simplification Act, 45 CFR: § 164.312 Technical safeguards, (b) Standard: Audit controls.

- NC Statewide Technical Architecture, Principles Practices and Standards
  - Security Domain 2.1.3 - Encrypt user-ids and passwords during transmission
  - Security Domain 3.1.10 - Secure transmission of sensitive data in both wired and wireless environments
  - Security Domain 4.1.6 - Establish change management processes and procedures to ensure that change itself does not introduce new security vulnerabilities

- NC Statewide Information Security Manual, Version No.1
  - Chapter 2 – Controlling Access to Information and Systems, Section 01:Controlling Access to Information and Systems
    - Standard 020105 - Controlling Access to Operating System Software
    - Standard 020106 - Managing Passwords
    - Standard 020112 - Controlling Remote User Access
    - Standard 020119 - Diagnostic and Configuration Port Controls
  - Chapter 3 – Processing Information and Documents, Section 02: Systems Operation and Administration
    - Standard 030203 - Controlling Data Distribution and Transmission
    - Standard 030206 - Managing System Operations and System Administration
    - Standard 030207 - Managing System Documentation
    - Standard 030208 - Monitoring Error Logs
    - Standard 030209 - Scheduling System Operations
    - Standard 030210 - Scheduling Changes to Routine System Operations
    - Standard 030211 - Monitoring Operational Audit Logs
    - Standard 030217 - Log-on Procedures
    - Standard 030218 - System Utilities
    - Standard 030219 - System Use Procedures
    - Standard 030221 - Corruption of Data
    - Standard 030223 - Controlling On-Line Transactions
  - Chapter 4 – Purchasing and Maintaining Commercial Software, Section 02:Software Maintenance and Upgrade
    - Standard 040202 - Upgrading Software
    - Standard 040206 - Operating System Software Upgrades
    - Standard 040207 - Support for Operating Systems
  - Chapter 6 – Combating Cyber Crime, Section 01:Combating Cyber Crime
    - Standard 060107 - Defending Against Hackers, Stealth- and Techno-Vandalism
  - Chapter 7 – Controlling E-Commerce Information Security, Section 01: E-Commerce Issues
    - Standard 070101 - Structuring E-Commerce Systems including Web Sites
    - Standard 070102 - Securing E-Commerce Networks
    - Standard 070104 - Using External Service Providers for E-Commerce;
  - Chapter 8 – Developing and Maintaining In-House Software, Section 01: Controlling Software Code
    - Standard 080101 - Managing Operational Program Libraries
    - Standard 080102 - Managing Program Source Libraries
    - Standard 080103 - Controlling Software Code during Software Development
    - Standard 080105 - Controlling Program Source Libraries
  - Chapter 8 – Developing and Maintaining In-House Software, Section 01: Software Development
    - Standard 080202 - Making Emergency Amendments to Software
    - Standard 080205 - Managing Change Control Procedures
    - Standard 080206 - Separating System Development and Operations

- Chapter 8 – Developing and Maintaining In-House Software, Section 03: Testing and Training
  - Standard 080302 - Using Live Data for Testing
- Chapter 13 – Detecting and Responding to IS Incidents, Section 04: Other Information Security Incident Issues
  - Standard 130408 - Risks in System Usage

- NC DHHS Policy and Procedures Manual, Section VIII - Security and Privacy, Security Manual
  - Applications Security Policy
  - Business Continuity and Disaster Recovery Plan Policy
  - Data Classification, Labeling and Access Control Policy
  - Information Security Management Policy
  - Information Systems Review and Auditing Policy
  - IT Inventory Management Control Policy
  - IT Operations Security Policy
  - Physical and Environmental Security Policy
  - Risk Management Policy
  - Security for Information Systems Contracts Policy
  - Security Training and Awareness Policy

- NC DHHS Security Standards
  - Administrative Security Standards
    - Information Classification Security Standard
    - Information Security Certification and Accreditation Standard
    - Information Security Change Management Standard
  - Application Security Standards
    - User Authorization & Authentication Standard
  - Network Security Standards
    - Digital Signature Standard
    - Telecommunications Security Standard
    - Encryption Standard
  - Physical Security Standards
    - Asset Inventory and Control Standard